IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

MONICA TOWNSEND, individually and on behalf of all others similarly situated, Plaintiff, v. HMG HEALTHCARE, LLC, Defendant.	)	CASE NO. 4:24-cv-00156 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Monica Townsend ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of all facts pertaining to herself and on information and belief as to all other matters, by and through the undersigned counsel, brings this Class Action Complaint against Defendant HMG Healthcare, LLC ("HMG" and/or "Defendant").

I. NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all others similarly situated, whose private and confidential personal identifying information ("PII") and/or protected health information ("PHI")—including their name, dates of birth, contact information, general health information, information regarding medical treatment, social security numbers and/or employment records—was compromised in a massive security breach of HMG's computer servers (the "Data Breach").

2. In a filing with the Texas Secretary of State, HMG reported that its Data Breach affected 75,000 Texans.[1] HMG did not report the number of non-Texans affected by the Data Breach.

3. As alleged herein, HMG's failure to implement adequate data security measures to protect its consumers' sensitive PII/PHI and proximately caused injuries to Plaintiff and the class members.

4. The Data Breach was the inevitable result of HMG's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving PII/PHI, HMG failed to ensure that it maintained adequate data security measures to protect PII/PHI from unauthorized third parties.

5. By collecting, using, and deriving a benefit from the PII/PHI of Plaintiff and Class Members, HMG assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. HMG had legal obligations and duties created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

7. HMG failed to adequately protect Plaintiff's and Class Members' PII/PHI and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII/PHI was compromised due to HMG's negligent and/or careless acts and omissions and its utter failure to protect the sensitive data it collected for its own pecuniary gain.

---

[1]Carly Page, *Texas-based care provider HMG Healthcare says hackers stole unencrypted patient data*, TechCrunch (Jan. 10, 2024), *accessible at* https://techcrunch.com/2024/01/10/hmg-healthcare-unencrypted-patient-data-breach/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAK4Idn1c2xTmugM_mvETdBDsD-psOfKv6x1l_VZHB83SEU7QojmDFYmF8mIz2Zp4TQSl6SoJy8nLFERmjvcva64U45Mpiqg_9F-nvqPuqD7UcbUywnwJaE3ScEgk3ClwoRlkH3wlIT0zYO1cDT7FtgOu9i83p5xU1RIeDpK9ul1W

8. Had HMG adequately designed, implemented, and monitored its network and servers, the Data Breach would have been prevented.

9. Had Plaintiff and Class Members known that HMG's data security was below industry standards, Plaintiff and Class Members would not have provided their PII/PHI to HMG or relied on HMG to protect that information.

10. As a result of HMG's inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at an imminent risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the cost of identity theft protection for the remainder of the lives of Plaintiff and Class Members (d) the loss of benefit of the bargain; (e) diminution of value of their PII/PHI; and (f) the continued risk to their PII/PHI, which remains in the possession of HMG, and which is subject to further breaches, so long as HMG fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI.

11. HMG failed to offer any meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach. In contrast to what has been frequently made available to consumers in other data breaches, HMG has not offered or provided any fraud insurance or basic identity monitoring services.

12. Moreover, The Data Breach was a direct result of HMG's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII/PHI. Despite discovering the Data Breach in November of 2023, HMG inexplicably failed to provide notice to impacted customers until December 29, 2023. As a result, HMG left a significant gap of time in which, unbeknownst to its customers, HMG knew of and could have notified its

customers of the Data Breach and advised its customers to take immediate remedial steps. Instead, HMG left its customers exposed.

13. Further, HMG has admitted that the Data Breach occurred in August of 2023, but failed to adequately monitor its servers, so HMG did not discover the Data Breach until November of 2023. As a result, HMG failed to close off this unauthorized actor from access to its customers' PII/PHI– leaving the door open for this unauthorized actor to continue to collect HMG's customers' PII/PHI for months.

14. Plaintiff and the class members seek to recover damages caused by HMG's negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment. Additionally, Plaintiff seeks declaratory and injunctive relief as a result of HMG's conduct, as discussed herein.

II. PARTIES

Plaintiff

15. Plaintiff Monica Townsend is a natural person and citizen and resident of Houston, Texas.

16. Plaintiff was a customer of HMG, which is a Texas-based care provider.

17. In exchange for receiving HMG's healthcare services, Plaintiff provided HMG with her PII/PHI as a regular part of HMG's business operations.

18. On December 29, 2023, HMG mailed Plaintiff a letter to notify her of the Data Breach and the impact to her PII/PHI (the "Notice Letter"). This Notice Letter stated that unauthorized actors gained access to and acquired files on HMG's servers, which included Plaintiff's PII/PHI. The Notice Letter did not identify what data was compromised, but HMG published a substitute notice in which it disclosed that the hackers compromised its customers medical records and personal information, including names, dates of birth, contact information,

general health information, information regarding medical treatment, social security numbers and/or employment records.[2]

19. Since learning of the Data Breach, Plaintiff has spent significant time in response to the Data Breach, heeding HMG's warnings to remain vigilant. She has spent time changing passwords on her accounts and monitoring her credit reports for unauthorized activity, which may take years to discover and detect.

20. Plaintiff plans on taking additional time-consuming but reasonable and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her credit reports for unauthorized activity.

21. As a result of HMG's conduct and omissions, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring her financial accounts for fraudulent activity, facing a present and continuing risk of fraud and identity theft, the lost value of her personal information, the cost of identity theft protection for the remainder of the lives of Plaintiff and Class Members, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their medical records for fraud or identify theft – particularly since the compromised information includes Social Security numbers.

22. The Data Breach has also caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that HMG has not been forthright about the cause and full scope of the PII/PHI compromised in the Data Breach.

[2]Derek Prince, *Privacy Update*, HMG Healthcare (last accessed Jan. 15, 2024), available at https://www.hmghealthcare.com/privacy-update/#additional-information.

23. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

24. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains in HMG's possession, is protected and safeguarded from future breaches.

Defendant

25. Defendant HMG is a Texas limited liability company with its headquarters in The Woodlands, Texas. Defendant may be served by and through its registered agent, Amarillo Corporate Services, LLC, located at 500 S. TAYLOR, SUITE 1100, LB 219, AMARILLO, TX 79105.

26. According to HMG's website, HMG provides a range of services, including memory care, rehabilitation and assisted living. HMG's website also says it serves approximately 3,500 patients and has several geographic locations throughout Texas and Kansas.[3]

III. JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interests and costs, and is a class action in which some members of the class are citizens of states different than Defendant HMG.

28. This Court has general personal jurisdiction over HMG, because HMG is a limited liability company which is incorporated in the State of Texas. Further, HMG is headquartered in The Woodlands, Texas.

[3] *Careers*, HMG Healthcare (last accessed Jan. 15, 2024), available at https://www.hmghealthcare.com/careers/.

29. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b) because this district is the judicial district in which a substantial part of the events and/or omissions giving rise to the claim occurred. Venue is also proper in this district pursuant to 28 U.S.C. § 1391(b) because this district is the judicial district in which the Defendant resides.

IV. FACTUAL ALLEGATIONS

30. Plaintiff and the proposed Class are consumers of HMG. HMG is a healthcare service provider.

31. As noted above, Plaintiff brings this class action against HMG for its failure to properly secure and safeguard personally indefinable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information has been compromised.

HMG was obligated to safely protect its customers PII/PHI.

32. Plaintiff and Class Members provided their PII/PHI to HMG with the reasonable expectation and mutual understanding that HMG would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. Plaintiff and Class Members' PII/PHI was provided to HMG in conjunction with the type of work HMG does in providing healthcare services. Upon information and belief, as a condition of providing healthcare services to its patients and customers, HMG required that each patient and customer sign a form authorizing the use and/or disclosure of their protected health information, pursuant to HIPAA.

34. In receiving the PII/PHI as part of its services, HMG assented and undertook legal duties to safeguard and protect the PII/PHI entrusted to them by Plaintiff and Class Members, in compliance with all applicable laws, including HIPAA.

35. HMG's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

36. However, HMG failed to secure the PII/PHI of the individuals that provided them with this sensitive information.

The HMG Data Breach

37. According to HMG's privacy update, in November 2023, HMG became aware of a data breach of personal health information related to residents and employees at HMG affiliated nursing facilities.[4]

38. According to HMG, HMG's investigation revealed that hackers gained access to its server and stole unencrypted files, which likely contained medical records and personal information, including names, dates of birth, contact information, general health information, information regarding medical treatment, social security numbers and/or employment records.[5]

39. However, HMG did not reveal any details of the root cause of the Data Breach, the vulnerabilities exploited, whether HMG's system is still unsecured, why HMG failed to detect the Data Breach for months, why HMG decided to wait almost two months inform impacted individuals after HMG first detected the Data Breach, or any remedial measures HMG was taking to ensure such a breach does not occur again. HMG still has not explained these details to Plaintiff or the Class Members who have a vested interest in ensuring that their PII/PHI remains protected.

40. HMG failed to take appropriate or even the most basic steps to protect the PII/PHI of Plaintiff and other class members from being disclosed.

[4] *Supra* n.2

[5] *Id.*

41. Though HMG claimed in their notice that they "took steps to investigate the incident fully, mitigate any potential harm… and protect against any further breaches,"[6] HMG failed to secure its network for months while the unauthorized user continued to exploit HMG's network vulnerabilities.

42. Moreover, HMG admits, without explanation, that it attempted to identify the specific data that was compromised but determined that such identification was not feasible.[7] Upon information and belief, HMG's inability to identify the specific compromised data is due to HMG's failure to maintain system logs, or its systems were so weak that the threat actors were able to evade or disable the logging.

43. Further, as HMG admits, the PII/PHI contained in the files accessed by cybercriminals was not encrypted or inadequately encrypted.[8]

Plaintiff and the class members have suffered as a result of the Data Breach.

44. PII/PHI is a valuable property right.[9] PII/PHI has measurable value as a commodity.[10] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[11] American companies are estimated to have spent over $19 billion on acquiring

---

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[10] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited January 16, 2023).

[11] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[12] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

45. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[13]

46. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

---

[12]U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[13]Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[14]Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[15]Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[16]*In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on January 16, 2023).

[17]*See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

47. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

48. One such example of criminals using PII for profit is the development of "Fullz" packages.[18] "Fullz" packages are products compiled by cross-referencing two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

49. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

[18]"Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

50. Further, criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

51. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

52. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

53. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[22]

---

[19]*See* https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach- reporting/index.html.

[20]*Id*.

[21]Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[22]Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

54. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[23]

55. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[24]

56. HMG was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as HMG does. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[25]

57. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear

[23]Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[24]*See* Maria Henriquez, *Iowa City Hospital Suffers PIIshing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-PIIshing-attack.

[25]Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

58. Once PII/PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and the class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of HMG's conduct. Further, the value of Plaintiff's and class members' PII/PHI has been diminished by its exposure in the Data Breach.

59. As a result of HMG's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII/PHI.

60. Plaintiff and the Class suffered actual injury from having PII/PHI compromised as a result of HMG's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that HMG obtained from Plaintiff; (b) violation of their privacy rights; (c) present and continuing risk arising from the identity theft and fraud; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (e) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; and (f) invasion of privacy.

61. Plaintiff brings this class action against HMG for HMG's failure to properly secure and safeguard PII/PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII/PHI had been compromised.

V. CLASS ACTION ALLEGATIONS

62. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Personal Information or PHI was compromised in the Data Breach occurring in August 2023, including all individuals who Defendant mailed notice to on or around December 29, 2023.

63. Excluded from the Classes are HMG's officers and directors, and any entity in which HMG has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of HMG. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

64. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

65. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 60,000 Members.

66. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether HMG unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII/PHI;

b) Whether HMG failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c) Whether HMG's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d) Whether HMG's data security systems prior to and during the Data Breach were consistent with industry standards;

e) Whether HMG owed a duty to Class Members to safeguard their PII/PHI;

f) Whether HMG breached their duty to Class Members to safeguard their PII/PHI;

g) Whether computer hackers obtained Class Members' PII/PHI in the Data Breach;

h) Whether HMG knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether HMG's conduct was negligent;

j) Whether HMG's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k) Whether HMG's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l) Whether HMG violated the Federal Trade Commission Act ("FTC Act");

m) Whether HMG violated the Health Insurance Portability and Accountability Act ("HIPAA");

n) Whether HMG was unjustly enriched to the detriment of Plaintiff and the Class;

o) Whether HMG failed to provide notice of the Data Breach in a timely manner; and

p) Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

67. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

68. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

69. Predominance. HMG has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from HMG's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

70. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for HMG. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

71. HMG has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

72. Likewise, particular issues under are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether HMG owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII/PHI;

b) Whether HMG's data security practices were reasonable in light of best practices recommended by data security experts;

c) Whether HMG's failure to institute adequate protective security measures amounted to negligence;

d) Whether HMG failed to take commercially reasonable steps to safeguard consumer PII/PHI; and

e) Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

73. Finally, all members of the proposed Classes are readily ascertainable. HMG has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by HMG.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE

74. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1–73 as if fully set forth herein.

75. HMG owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in their possession, custody, or control.

76. HMG knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. HMG knew, or should have known, of the vast uptick in data breaches in recent years. HMG had a duty to protect the PII/PHI of Plaintiff and Class Members.

77. Given the nature of HMG's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, HMG should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which HMG had a duty to prevent.

78. HMG breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

79. It was reasonably foreseeable to HMG that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

80. But for HMG's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

81. As a result of HMG's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the present and continuing risks of medical identity theft they face and will continue to face; (viii) the cost of identity theft protection for the remainder of the lives of Plaintiff and Class Members and (ix) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

82. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1–73 as if fully set forth herein.

83. HMG's duties arise from, in part due to its storage of certain medical information, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

84. HMG's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as HMG, of failing to employ reasonable measures to protect and secure PII/PHI.

85. HMG's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

86. HMG is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

87. HMG violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. HMG's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

88. HMG's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

89. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

90. The harm occurring because of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

91. It was reasonably foreseeable to HMG that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

92. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of HMG's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including but not limited to the cost of identity theft protection for the remainder of the lives of Plaintiff and Class Members, which is necessary to protect against the present and continuing risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

93. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1–73 as if fully set forth herein.

94. Plaintiff and Class members either directly or indirectly gave HMG their PII/PHI in confidence, believing that HMG – a healthcare provider – would protect that information. Plaintiff and Class members would not have provided HMG with this information had they known it would not be adequately protected. HMG's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between HMG and Plaintiff and Class Members. Moreover, a fiduciary relationship existed between HMG and Plaintiff and the Class Members by virtue of HMG's provision of healthcare services to Plaintiff and the Class Members, which included a duty to ensure that Plaintiff's and the Class Members' PHI remained confidential.

95. In light of this relationship, HMG must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

96. HMG breached its fiduciary obligations by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI of Plaintiff and Class Members it collected.

97. As a direct and proximate result of HMG's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in HMG's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

98. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1–73 as if fully set forth herein.

99. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

100. Plaintiff and Class Members conferred a monetary benefit upon HMG in the form of monies paid for healthcare services or other services.

101. HMG accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. HMG also benefitted from the receipt of Plaintiff's and Class Members' PII/PHI.

102. As a result of HMG's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

103. HMG should not be permitted to retain the money belonging to Plaintiff and Class Members because HMG failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

104. HMG should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
BREACH OF IMPLIED CONTRACT

105. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1–73 as if fully set forth herein.

106. HMG required Plaintiff and Class Members to provide, or authorize the transfer of, their PII/PHI in order for HMG to provide services. In exchange, HMG entered into implied contracts with Plaintiff and Class Members in which HMG agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII/PHI and to timely notify them in the event of a data breach.

107. Plaintiff and Class Members would not have provided their PII/PHI to HMG had they known that HMG would not safeguard their PII/PHI, as promised, or provide timely notice of a data breach.

108. Plaintiff and Class Members fully performed their obligations under their implied contracts with HMG.

109. HMG breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII/PHI and by failing to provide them with timely and accurate notice of the Data Breach.

110. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of HMG's breach of its implied contracts with Plaintiff and Class Members.

VII. JURY DEMAND

111. Plaintiff demands a trial by jury on all claims so triable.

VIII. PRAYER

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b. For equitable relief enjoining HMG from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI;

c. For equitable relief compelling HMG to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the

Data Breach;

d. For an order requiring HMG to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

Dated: January 16, 2024

Respectfully submitted,

By: /s/*Bruce W. Steckler*

Bruce W. Steckler
TX Bar No. 00785039
bruce@swclaw.com
Kaitlyn M. Coker
TX Bar No. 24115264
kcoker@swclaw.com
Paul D. Stickney, of Counsel
TX Bar No. 00789924
judgestick@gmail.com
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
Fax: (972) 387-4041

John G. Emerson, Jr.
TX Bar No. 06602600
jemerson@emersonfirm.com
EMERSON FIRM, PLLC

2500 Wilcrest, Suite 300
Houston, TX 77042
Tel: (800) 551-8649
Fax: (501) 286-4649

John A. Yanchunis
TX Bar No. 22121300
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS